REMARKS

In the Office Action under reply, claims 1-3, 5-8, 10-13, 15-18, 20-23 and 25, all the claims remaining in this application, were rejected under 35 USC 103 as being unpatentable over the combination of Rosner (U.S. Patent 6,636,968), Kato (6,381,331) and Schneier ("Applied Cryptography"). It is respectfully submitted that the claims present in this application are patentably distinct over this combination for the reasons now discussed.

Claim 1 is directed to a digital data delivery method for delivering digital data to specific destinations, by which digital data is encrypted using an encryption key, respective pieces of key information used to decrypt the encrypted digital data are generated "by dividing said encryption key by a division pattern unique to each of said specific destinations and said division pattern based on the content of said digital data," and the encrypted digital data as well as the respective pieces of key information are delivered over different routes to the specific destinations whereat the respective pieces of key information are used to restore the encryption key which, in turn, is used to decrypt the digital data. In comparing claim 1 to the combination of Rosner, Kato and Schneier, the Examiner recognized that Rosner does not disclose Applicants' claimed features of: (1) "generating the pieces of key information by dividing the encryption key by a unique division pattern;" (2) the "division pattern based on the content of said digital data;" and (3) delivering the key information over a plurality of delivery routes which differ from each other and from the delivery route of the encrypted digital data. However, the Examiner contends that Kato teaches that "the encryption keys used to encrypt the content should be prepared for each content (see Kato column 10, lines 37-52)" and that when Kato is combined with Rosner, the resultant would teach the use of a separate encryption key for each content.

At page 3 of the Office Action under reply, the Examiner contends that Rosner "generate[s] a plurality of pieces of key information on the basis of said encryption key... see Rosner column 3, lines 48-57)." While, it is not clear if Rosner generates pieces of key information on the basis of an encryption key, it is undeniable that Rosner fails to suggest "dividing said encryption key by a division pattern." Turning to the referenced portion of Rosner, Rosner states that a session key to 221 "is based upon a secret key x ... and public keys 251a, 261a and 271a ." Rosner states that partial keys 225, 226 and 227 are generated; and here too, it is not clear if these partial keys are generated on the basis of an encryption key -- but it is clear that these partial keys will not be generated "by dividing said encryption key by a [unique] division pattern."

The Examiner relies upon Schneier as teaching that key information should be delivered over different channels; and Applicants agree that Figure 8.2 at page 177 of Schneier teaches this feature.

The Examiner further relies upon Schneier as allegedly teaching "that the key should be split using random numbers, which would be unique for each splitting (see Schneier pages 70-71, section 3.6 Secret Splitting)." Applicants do not agree with this interpretation of Schneier.

It is respectfully submitted that neither Kato nor Schneier suggests features (1) or (2) of Applicants' claim 1, mentioned above, as will now be explained. Section 3.6 (Secret Splitting) of Schneier divides a **message** into pieces by exclusive or-ing the message with two, three or more random-bit strings R, S, T, U, ... The result of this exclusive or operation is an encrypted message. There is no use of an encryption key to encrypt the message because there is no need to do so. Thus, there is no splitting of an encryption key using random numbers, as suggested by the Examiner. Not only is there no "key" to be split, but Schneier specifically states, in his last

sentence of section 3.6, "Remember, M isn't being split in the normal sense of the word; it is being XORed with random values." Thus, even if one attempted to construe Schneier's "message" as corresponding to Applicants' encryption key, Schneier teaches away from splitting the message (or encryption key) into respective pieces. Accordingly, one of ordinary skill in the art, after reading and understanding Schneier and recognizing that an input message, or digital data, can be encrypted by XORing that digital data with a number of random-bit strings, would not be enabled thereby to generate respective pieces of key information by dividing an encryption key by a unique division pattern. There simply is no suggestion in Schneier to divide or split anything, much less an encryption key. See the last sentence of Schneier's section 3.6, which clearly teaches away from "dividing said encryption key by a [unique] division pattern."

Kato apparently was relied upon as an alleged teaching of feature (2) of claim 1, mentioned above. It is respectfully submitted that Kato does not provide such a teaching. Kato divides digital data into blocks and uses a first key K1 to encode some of the blocks and a second key K2 to encode the remaining blocks (see column 1, lines 53-63 and column 4, lines 24-27 of Kato). The user uses key K1 to decrypt sample data blocks and key K2 to decrypt paid data blocks. The user is provided with key K2 only after he agrees to purchase the information that can be decrypted only with key K2. Column 10, lines 46-48 of Kato state, "The keys K1, K2 and Tk are prepared in units of contents, and the keys K2 and Tk are changed at predetermined time intervals." Admittedly, this description in Kato is less than clear. If keys K1 and K2 are based on the content of the digital data, one would expect that, with respect to the content database shown in Kato's Figure 12, key K1 should be the same for all downloaded content X, key K11 should be the same for all downloaded content Y, etc. But, this is not disclosed or suggested by Kato. That Kato fails to suggest keys that are based on the content of the digital data is

reinforced by the fact that key K2 is changed "at predetermined time intervals," which has nothing to do with content.

In light of the aforenoted deficiencies found in Rosner, Schneier and Kato, the resultant combination of these three references is not sufficient to teach the feature of

> "generating a plurality of pieces of key information on the basis of said encryption key, respective pieces of said key information being generated by dividing said encryption key by a division pattern unique to each of said specific destinations and said division pattern based on the content of said digital data"

as recited in claim 1. The manner in which the pieces of key information are generated cannot be ignored. The recitation of "dividing said encryption key by a division pattern" is understood in accordance with the common meaning of these words. See, for example, paragraph [0095] of published application 2002/0106086, which is the publication of the instant application. Accordingly, one of ordinary skill in the art, after reading and understanding Rosner, Schneier and Kato would not be enabled by the cumulative teachings of these references to make and use the digital data delivery method defined by Applicants' claim 1. Therefore, the withdrawal of the rejection of this claim as being obvious in view of the cited prior art references is respectfully solicited.

Claims 2, 3, 5-8, 10-13, 15-18, 20-23 and 25 are unobvious over the combination of Rosner, Schneier and Kato because these claims call for the generation of pieces of key information, passkeys or passkey information on the basis of the encryption key by "dividing said encryption key by a division pattern unique to each of said specific destinations and said division pattern based on the content of said digital data." That this feature of generating pieces of key information, passkeys or passkey information is patentably distinct over the cited prior art

has been discussed above. Accordingly, the withdrawal of the rejection of claims 2, 3, 5-8, 10-13, 15-18, 20-23 and 25 is respectfully solicited.

Statements appearing above in respect to the disclosures in the cited references represent the present opinions of the undersigned attorney, and in the event the Examiner disagrees with any of such opinions, it is respectfully request into that the Examiner specifically indicate those portions of the references providing the basis for a contrary view.

Claims 1-3, 5-8, 10-13, 15-18, 20-23 and 25 are in condition for allowance. An early notice to that effect is respectfully urged.

Please charge any additional fees that may be needed, and credit any overpayment to our Deposit Account No. 50-0320.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By: 
William S. Frommer
Reg. No. 25,506
(212) 588-0800